**1.XSS(Cross Site Scripting)**

When we Edit or Add some person’s information, we can write some script, and it does really work!

In the textbox, we write the script:

<script>alert(‘hello world’)</script>

And this message will pop out when we step into this page.

**2.Insufficient authentication/permissions not checked(1)**

I am User 4 and currently only user3 share his contact with me. The logic of this website should be: if some other people who does not share his contact with me, then I should not be allowed to view his contact. But I found I can still view other people’s contact even if he did not share his contact with me.

I only need to visit the link: <https://ggbaker.ca/security/friends/user3/>, and change the /user3/ to /user1/, then I can view user1’s contact without any authentication.

**3.Insufficient authentication/permissions not checked(2)**

I am user1, and now already shared my contact with all of user2, user3 and user4. But In the home page,

When I click the ‘share my contacts with a friend’ -- When I attempt to launch a request, but I should not do so, after check from the server, this request should have been blocked, otherwise, while I step into that page, I will be deadly stuck inside.

That is, when I step into <https://ggbaker.ca/security/friends/new> page after I click that button, whoever I choose, it will tell me that I already choose him, or I can not choose myself. There is no ‘home’ button, or ‘return back’ button, so user will not be able return back to any other page.(maybe the developer can just put some more buttons here, instead of making some modification in the logic of server side.)

**4.CSRF**

While I am in the people(contact) edit page, then enter the following script in the textbox,

<form action="/security/friends/user3/from-user1/delete" method="post"><input type="hidden" name="csrfmiddlewaretoken" value="aIJHkEk5PhmrDXJnXWnm6Dp5TDYHBE9bDIomA5YzG5U9h3MnUPLF3aORBD6mDgzT">

<input type="text" />

<input type="submit" value="Search" />

</form>

Then the textbox will be look like a search bar, when I clean the ‘search’ button, it will send the delete post and we will successfully unshared contact with user3.

**5.Other Inappropriately logic 1**

In the login request, we can see exact password in the post data via chrome network tool. It may be better if there are some technique(e.g., hash with salt and etc.) to keep it more secretly.

**6.Other Inappropriately logic 2**

I am now user 1, The website logic will not allow me to add myself as a friend,

But I can still view my own contacts via this link, which seems weird, because we can see this link path is under ../friends/…

<https://ggbaker.ca/security/friends/user1/>

This implementation logic is a contradiction.